Enclosure 23 to ET 07-0022

Applicability of RTCA DO-254, Revision 0

MAIN STEAM & FEEDWATER ISOLATION SYSTEM (MSFIS) CONTROLS REPLACEMENT

APPLICABILITY OF RTCA DO-254

REVISION 0

PROJECT MANAGER - GREGG CLARKSON
MANAGEMENT SPONSOR - PATRICK GUEVEL
EXECUTIVE SPONSOR - TERRY GARRETT

Wolf Creek Nuclear Operating Corporation
PO Box 411
1550 Oxen Lane, NE
Burlington, KS 66839

Table of Contents

1 Introduction

1.1 Purpose

The purpose this document is to provide information on the applicability of RTCA DO-254, "Design Assurance Guidance for Airborne Electronic Hardware," to the Advanced Logic System (ALS) Main Steam and Feedwater Isolation System (MSFIS) project field programmable gate array (FPGA) design process.

1.2 References

1.2.1 IEEE Std 603-1998, IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations

1.2.2 IEEE Std 7-4.3.2-1993, IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations

1.2.3 RTCA DO-254/EUROCAE ED-80, Design Assurance Guidance for Airborne Electronic Hardware

1.2.4 Regulatory Guide 1.152, Criteria for Use of Computers in Safety Systems of Nuclear Power Plants, Rev. 2

2 DO-254 Applicability

The upgrade of the MSFIS is implemented using the ALS. The ALS is a rack-based hardware system consisting of several circuit cards which contain both analog and digital devices. In the ALS design, all of the functions have been allocated to hardware; none of the system functionality has been implemented in software. Each circuit card in the ALS is controlled by an FPGA; there are no processors, microcontrollers, CPU elements or microcode. None of the FPGA's contain any processor cores or any type of Arithmetic Logic Unit (ALU), in fact, the design could be implemented using just logic chips such as 7400 series OR-gates, AND-gates, latches, etc. The FPGA logic design is accomplished by using a Hardware Description Language (HDL), and the basic design element, which eliminates the need for any processors or application software, is the finite state machine. The particular FPGA implemented in the ALS utilizes basic unconnected logic elements which are then interconnected using flash memory programming to configure the device, similar to the wiring on a Printed Circuit Board (PCB). Logic design software tools are used in the logic development process, as well as in the circuit design, board design, and build processes. These software tools are controlled under configuration management by the controls vendor. The software tools utilized in this project were chosen and confirmed suitable for use by the controls vendor using the following criteria: 1) implementing V&V activities which detect possible defects in the software tools, 2) a review of operating experience of the tool(s), and 3) corrective action program(s) implemented by the tool vendor.

Because there are similarities between this type of hardware design and a PLC or microcontroller based I&C instrument design, the guidance of Regulatory Guide 1.152 and IEEE Std 7-4.3.2-2003 has been followed where applicable and WCNOC has also structured the V&V Plan on elements of IEEE Std 7-4.3.2. For example, the following IEEE Std 7-4.3.2 requirements have been met: V&V Plan, Configuration Management Plan, Requirements Traceability Matrix, System Reliability Analysis, Failure Modes and Effects Analysis, and EMC qualification. However, there are also some requirements and guidance for software-based systems which are not appropriate to an ALS-type FPGA design. WCNOC notes the following quote:

> "HDL design representations use coded text based techniques that are similar in appearance to those used for software representations. This similarity in appearance can mislead one to attempt to use software verification methods directly on the design representation of HDL or other equivalent hardware specification languages." [RTCA DO-254/EUROCAE ED-80: "Design Assurance Guidance for Airborne Electronic Hardware" (endorsed by FAA AC 20-152)]

Additionally, there is no guidance within IEEE Std 7-4.3.2 for a hardware-only logic system based on FPGAs. DO-254 applies specifically to an FPGA based system. It was developed because safety critical flight equipment vendors were attempting to use DO-178 (a software standard which is similar to IEEE Std 7-4.3.2) for these hardware systems which are common in flight controls, and the resulting QA requirements and procedures were inappropriate.

The development of the system does utilize software tools as discussed above, however those tools are treated appropriately as to ensure defects are not injected into the design. The FPGA development tools are utilized as tools for implementing the hardware design in the same way as the software tools used for developing the PCB or a discrete logic design. The key point to the application of logic design tools in this design is that the outputs of the tools are independently validated to ensure that the tools do not cause any design errors.

The controls vendor's design flow and design QA processes are structured in accordance with DO-254. The Nutherm International Dedication Report will describe how these activities are employed to meet DO-254 and the intent of the criteria described in IEEE Std 7-4.3.2, Section 5.3.2. As proscribed by Section 5.3.2, the software tools being used on this project are used in a manner such that defects not detected by the software tool will be detected by V&V activities. The Dedication Report will also address tool operating experience, also per Section 5.3.2.

3 IEEE 7-4.3.2 Requirements Cross Referenced to DO-254

Assumptions:

1. *The ALS MSFIS is considered a DO-254 "Complex Item"*
2. *DO-254 Design Assurance Level A is applicable*

3.1 Table 1—Mapping of IEEE Std 7-4.3.2-2003 Quality Requirements to DO-254

IEEE Std 7-4.3.2-2003 requirement	DO-254 requirement
5.3 Quality – Life Cycle Process	3.0 Hardware Design Life Cycle
5.3.1 Software Development – QA Plan	4.0 Planning Process
5.3.2 Software Tools	4.2 Planning Process 7.2 Configuration Management 7.2.4 Change Control 10.1.5 Hardware Configuration Management Plan 11.4 Tool Assessment And Qualification
5.3.3 Verification and Validation	6.0 Validation and Verification Process
5.3.4 Independent V&V	4.2 Planning Process 8.0 Process Assurance 10.1.4 Hardware Verification Plan Appendix A Appendix B
5.3.5 Software Configuration Management	7.0 Configuration Management Process
5.3.6 Software Project Risk Management	1.6 Complexity Considerations 3.1 Hardware Design Life Cycle Processes
5.4 Equipment Qualification	6.3 V&V Methods
5.4.1 Computer System Testing	6.3.1 Test
5.4.2 Qualification of Existing Commercial Computers	11.0 Additional Considerations 11.1 Use of Previously Developed Hardware 11.2 Commercial-Off-The-Shelf (COTS) Component Usage
5.5 System Integrity	2.3.3 Qualitative Assessment of Hardware Design Errors and Upsets
5.5.1 Design for Computer Integrity	2.3.1 Hardware Safety Assessment Considerations
5.5.2 Design for Test and Calibration	2.3.1 Hardware Safety Assessment Considerations
5.5.3 Fault Detection and self-diagnostics	2.3.1 Hardware Safety Assessment Considerations 2.3.4 Design Assurance Considerations for Hardware Failure Condition Classification
5.6 Independence	2.3.4 Design Assurance Considerations for Hardware Failure Condition Classification
5.15 Reliability	2.3.4 Design Assurance Considerations for Hardware Failure Condition Classification

3.2 Table 2—Mapping of IEEE Std 603-1998 to IEEE Std 7-4.3.2-2003 and DO-254 (from Table A.1 of IEEE 7-4.3.2 Annex A)

IEEE Std 603-1998 criteria	IEEE Std 7-4.3.2-2003 additional requirements	DO-254 requirements
4. Safety system design basis	Safety system design basis, Annex B	Hardware Safety Assessment 2.3
5. Safety system criteria	Annex B	Hardware Design Process 5.0, Appendix B
5.1 Single-failure criterion	None	Hardware Safety Assessment 2.3.1, Appendix B
5.2 Completion of protective action	None	None
5.3 Quality	Software development (5.3.1) Software tools (5.3.2) Frication and validation (5.3.3) Independent V&V (IV&V) requirements (5.3.4) Software configuration management (5.3.5) Software project risk management (see 5.3.6), Annex D and Annex F	Hardware Development - 3.0, 4.0, 5.0, V&V – 6.0, Config Mgmt – 7.0,\ Process Assurance – 8.0,
5.4 Equipment qualification	Testing software and diagnostics (see 5.4.1) Qualification of existing commercial computers (5.4.2), Annex C	Qualification of COTS components – 11.0
5.5 System integrity	Design for computer integrity (5.5.1) Design for test and calibration (5.5.2) Fault detection and self-diagnostics (5.5.3), Annex B and Annex C	Detailed Design Process 5.3.2
5.6 Independence	Independence (5.6), Annex E	Appendix A, Appendix B
5.7 Capability for test and calibration	None	Detailed Design Process 5.3.2
5.8 Information displays	None	None
5.9 Control of access	None	None
5.10 Repair	None	None
5.11 Identification	Identification (5.11)	None
5.12 Auxiliary features	None	None
5.13 Multi-unit stations	None	None
5.14 Human factor considerations	None	None

IEEE Std 603-1998 criteria	IEEE Std 7-4.3.2-2003 additional requirements	DO-254 requirements
5.15 Reliability	Reliability (5.15) , Annex F	Hardware Safety Assessment 2.3.1, Conceptual Design 5.2.2, V&V Analysis 6.3.2, Hardware Design Data 10.3.1, COTS Components 11.2.1
6. Sense and command feature—Functional design requirements	None	None
7. Execute feature—Functional design requirements	None	None
8. Power source requirements	None	None